	Application No.	Applicant(s)
Notice of Allowability	10/716,731	LEE ET AL.
	Examiner	Art Unit
	Samson B. Lemma	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 11/20/2007*.

2. ☒ The allowed claim(s) is/are *1-12, 14-15, 17 and 19-20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None of the:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

       3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

        Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08),
   Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☒ Interview Summary (PTO-413),
   Paper No./Mail Date *11/8/2007* .

7. ☐ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

DETAILED ACTION

1.   The request filed November 20, 2007 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/716,731 is acceptable and an RCE has been established.

Each and every independent claim, namely **claim 1, 5 and 7** is/are amended.

Claims **13, 16 and 18** are canceled previously. Thus claims **1-12, 14-15, 17 and 19-20** are pending/examined.

2.   On November 8, 2007 Applicant's representative, Lindsay G. McGuinness, Reg. No. 38,549 and examiner discussed the limitation recited in the indepenent claims and the corresponding prior arts (references) used for rejecting the claims. Furthermore the parties discussed, how the indepenent claims should be amended to overcome the ground of rejection set forth in the previous office action, including the comment suggested by the examiner on the previous advisory office action. Accordingly, both parties (Examiner and applicant's representative) agreed the language of claims that would clarify the respective indepenent claims and overcome the ground of rejection. Examiner suggested that further search, consideration and approval from the supervisor is required before determining whether or not the application is allowable.

Allowable Subject Matter

3.   **Claims 1-12, 14-15, 17 and 19-20 are allowed.**

4.   The following is an examiner's statement of reasons for allowance:

Referring to the previous independent claims 1 and 5 Jari, the primary reference on the record, discloses **a method for re-establishing secure communications between a node and an endpoint node including the steps**

of:[Abstract and paragraph 0037] (As it is described on the abstract, "When a restoration of power to the security gateway is detected following a power failure, the controller 6 retrieves the latest security association database from the memory 7 and injects it into the volatile memory 5 whose contents were lost during the power failure. The security gateway 2 then restore secure communication with external users.")

- **Copying,** ["retrieve" see paragraph 0013 and see "injects" on the abstact] **responsive to a reset at the node,** ["restoration of power to the node" see paragraph 0013, abstract and 0005] **a set of security associations stored in a memory** ["a volatile memory for containing a security association database comprising a plurality of security associations, see paragraph 0005] **to a working set of security associations** ["security association which is injected on the volatile memory shown on figure 1, ref. Num 5]

Furthermore Jari on paragraph 0032 **discloses,** the following, "the security gateway 2 controls communication between external or mobile users and the VPN 1 in accordance with the pre-negotiated security associations **in a manner which is known and which will therefore not be described further and as indicated on paragraph".** The manner, which is known, includes the **IKE SA** as described on the secondary reference on column 0024-0026]. **On paragraph 0025, the following has been described.** "To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, **which have been digitally signed by a trusted third party certificate authority 115.** Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPSec SA". And on paragraph 0026, the following has been described. "When this is done, the IPSec

SA has been established, and the first 110 and second 114 gateway computers **store the SA in respective Security Association Databases (SADs) 116, 118.**" And nodes digitally signed **by a trusted third party are trusted nodes** and meets the limitation of "**wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;**

Jari does not explicitly discloses

- **wherein the set of security associations includes only the security associations for a set of trusted endpoints nodes, the set of trusted endpoints nodes determined according to a security association re-use policy of the node;**
- **Receiving, at the node, a communication from the endpoint node**
- **Determining whether a security association for the endpoint node is included in the working set of security associations;**
- **responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node.**

However, in the field of endeavor **Mercer, the secondary reference on the record discloses,**

- **wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;[paragraph 0025-0026]** *("In order to establish the IPSec SA, the first 110 and second 114 gateway computers must agree upon an encryption algorithm, an authentication algorithm, and have a shared session key. The first 110 and*

second 114 gateway computers must also provide each other with the appropriate

SPI value 310, 410 to include in the IPSec header portion 304, 404. And all these

information is interpreted as a security association re-use policy of the node. When

this is done, the IPSec SA has been established, and the first 110 and second 114

gateway computers store the SA in respective Security Association Databases

(SADs) 116, 118." Furthermore, Examiner would also like to point out that, Mercer

on paragraph 0025, discloses the following. "To establish an IKE SA, the first 110

and second 114 gateway computers exchange digital certificates, which have

been digitally signed by a trusted third party certificate authority 115. Thereafter,

when the IKE session becomes active, the first 110 and second 114 gateway

computers can establish the IPSec SA". And on paragraph 0026, the following has

been described. "When this is done, the IPSec SA has been established, and the

first 110 and second 114 gateway computers store the SA in respective Security

Association Databases (SADs) 116, 118." And nodes digitally signed by a trusted

third party are trusted nodes and meets the limitation of "wherein the set of

security associations includes only the security associations for endpoints nodes

that are trusted by the node. Therefore the combinations of these two paragraph

meets the limitation recited as **"the set of trusted endpoint nodes determined**

according to a security association re-use policy of the node.")

●   **Receiving, at the node** *[paragraph 0026 and paragraph 0030] (The*

second gate way computer 114/node, receives the Ipsec datagram 300, 400], **a**

communication from the endpoint node. */[the first gateway computer*

110/endpoint node, encrypts each IP datagram 200, forms a new IPSec

datagram 300,400 and send it to the second gateway computer)

●   **Determining whether a security association for the endpoint node is**

included in the working set of security associations; *[paragraph 0026 and*

paragraph 0030], (When the second gateway computer 114 receives the IPSec

datagram 300,400, which is sent from the gateway computer 110/endpoint node,

it/the second gateway computer 114/node, looks up the IPSec SA in the SAD

118/working set of security associations/security association Databases, shown

on figure 1, ref. Num 118)

- **responsive to a determination that the security association for the**

endpoint node is in the working set of security associations, using the

security association to process the communication from the endpoint

node. *(Paragraph 0026 and paragraph 0030] (It looks up the IPSec SA in its SAD*

118, and this is done in order to determine that the security association for the

endpoint node/gateway computer 110/ is already in the SAD 118/working set of

security associations/security association Databases and once the determination

is made, properly processes the datagram, and forwards it to the second

individual computer workstation 112-1). And,

Referring to the previous independent claim 7, **Jari, the primary**

reference on the record discloses a network device including:

- **Security association logic** [Abstract, figure 1, ref. 4 and paragraph

0032] *(the security gateway 2 contains a CPU 4 having a volatile memory 5 in*

which stored, among other things, a security association database controlling

secure communication between the network and external users), **coupled to the**

non-volatile memory, [figure 1, ref. Num 7, abstract] **for applying security**

associations to communications received by the network device [Abstract]

(a controller 6 periodically stores the security association database in a disk

memory 7 or other nonvolatile memory)

- **The security association logic** [Figure 1, ref. Num 4] **including**:

    - **a first memory comprising at least one entry, the entry comprising an endpoint identifier for each endpoint communicating with the network device and a security association associated with the each endpoint**; [paragraph 0032] (*The security gateway 2 comprises a central processing unit (CPU) 4 in the form of one or more programmable data processors controlled by a stored program. The CPU 4 includes a volatile memory 5, for example in the form of random access memory (RAM), for storing temporary values generated during operation of the CPU 4 in accordance with normal programmed data processor or computer techniques. During normal operation of the security gateway 2, the volatile memory contains, among other things, a security association database (SAD) in the form of a plurality of security associations. For example, each security association may comprise a **header sequence number, encryption and authentication algorithms and parameters, and lifetime information for the security association**. The security gateway 2 controls communication between external or mobile users and the VPN 1 in accordance with the pre-negotiated security associations in a manner which is known and which will therefore not be described further.*) and

    - **A second memory [Figure 1, ref. Num 7], storing a subset of data of the first memory, the subset of data selected according to the list of trusted endpoints** [Figure 1, ref. Num 5] *(The security gateway 2 contains a CPU 4 having a volatile memory 5/first memory, in which is stored, among other things, a security association database for controlling secure communications between the network and external users. A controller 6 **periodically stores** the*

security association database in a disk memory 7 or other nonvolatile

memory/second memory)

Furthermore Jari on paragraph 0032 **discloses,** the security gateway 2

controls communication between external or mobile users and the VPN 1 in

accordance with the pre-negotiated security associations **in a manner which is**

known and which will therefore not be described further and as indicated

on paragraph". The manner, which is known, includes the **IKE SA** as described

on the secondary reference on column 0024-0026]. **On paragraph 0025, the**

following has been described. "To establish an IKE SA, the first 110 and

second 114 gateway computers exchange digital certificates, **which have been**

digitally signed by a trusted third party certificate authority 115.

Thereafter, when the IKE session becomes active, the first 110 and second 114

gateway computers can establish the IPSec SA". And on paragraph 0026, the

following has been described. "When this is done, the IPSec SA has been

established, and the first 110 and second 114 gateway computers **store the SA**

in respective Security Association Databases (SADs) 116, 118." And nodes

digitally signed **by a trusted third party are trusted nodes** and meets the

limitation of **"wherein the set of security associations includes only the**

security associations for endpoints nodes that are trusted by the node;

Jari does not explicitly discloses

A first memory comprising a list of trusted endpoints, the list of

trusted endpoint being determined according to the security association re-use

policy of the network device;

However, in the field of endeavor **Mercer, the secondary reference on**

the record discloses,

- **A first memory comprising a list of trusted endpoints, the list of trusted endpoint being determined according to the security association re-use policy of the network device;**[Paragraph 0025-0026] ("In order to establish the IPSec SA, the first 110 and second 114 gateway computers must agree upon an encryption algorithm, an authentication algorithm, and have a shared session key. The first 110 and second 114 gateway computers must also provide each other with the appropriate SPI value 310, 410 to include in the IPSec header portion 304, 404. And all these information is interpreted as a security association re-use policy of the node. When this is done, the IPSec SA has been established, and the first 110 and second 114 gateway computers store the SA in respective Security Association Databases (SADs) 116, 118." Furthermore, Examiner would also like to point out that, Mercer on paragraph 0025, discloses the following. "To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, which have been digitally signed by a trusted third party certificate authority 115. Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPSec SA". And on paragraph 0026, the following has been described. "When this is done, the IPSec SA has been established, and the first 110 and second 114 gateway computers store the SA in respective Security Association Databases (SADs) 116, 118." And nodes digitally signed by a trusted third party are trusted nodes and meets the limitation of "wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node. Therefore the combinations of these two paragraphs meets the limitation recited as "the set of trusted endpoint nodes determined according to a security association re-use policy of the node.")

- However **the combination of Jari and Mercer** does not disclose the following functional limitation which was added to the respective independent claims when RCE is filled, **"wherein the security association re- use policy controls the set of trusted endpoints to comprise <u>only end-points that are known to the node and communicate with the node on a regular basis only end-points that are known to the node and communicate with the node on a regular basis.</u>"**

  None of the prior art of record taken singularly of in combination teaches a method for re-establishing secure communications between a node and endpoint node, with the above underlined/bolded functional limitation together with the other limitation recited in respective independent clams . For this reason, independent claims **1, 5 and 7** are found to be novel and are allowed.

5.   The dependent **claims** which are dependent on the above **independent claims 1, 5 and 7** being further limiting to the independent claims, definite and enabled by the specification are also allowed.

  Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
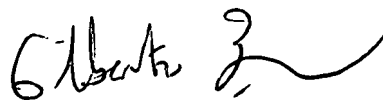
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
11/23/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100